Aula 13

DOMÍNIOS EUCLIDIANOS

META

Estabelecer o conceito de domínio euclidiano.

OBJETIVOS

Reconhecer domínios euclidianos.

Aplicar as propriedades dos domínios euclidianos na resolução de problemas.

PRÉ – REQUISITO

Aula 10.

INTRODUÇÃO

O algoritmo da divisão em $\mathbb{Z}$, estudado na aula 2, em essência, diz que em $\mathbb{Z}$, podemos fazer a divisão de um elemento a por outro b (não nulo) obtendo um "resto pequeno", ou mais precisamente, um resto cujo valor absoluto seja menor do que o valor absoluto de b. Um domínio euclidiano nada mais é do que um domínio que tem um algoritmo similar ao de Euclides em $\mathbb{Z}$. Aliás, os inteiros munidos do algoritmo de Euclides é um exemplo de domínio euclidiano.

O CONCEITO DE DOMÍNIO EUCLIDIANO

Definição 1. Dizemos que um domínio D é euclidiano, se existe uma função $\psi: D\backslash\{0\} \longrightarrow \mathbb{N}$ satisfazendo as seguintes propriedades:

i) $\forall a, b \in D, b \neq 0$, existem $q, r \in D$ tais que $a = bq + r$ e $r = 0$ ou $\psi(r) < \psi(b)$.

ii) $\forall a, b \in D\backslash\{0\}$, temos $\psi(a) \leq \psi(ab)$.

Exemplo 1. Sejam $D = \mathbb{Z}$ e $\psi = |\ \ |$ (a função valor absoluto, $|\ \ |: \mathbb{Z}\backslash\{0\} \longrightarrow \mathbb{N}$). Então, o algoritmo de Euclides afirma que dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existem $q, r \in \mathbb{Z}$ tais que $a = bq + r$ e $0 \leq r < |b|$. Notemos que a condição $0 \leq r < |d|$ é equivalente a $r = 0$ ou $|r| < |d|$. Dados $a, b \in \mathbb{Z}\backslash\{0\}$, como $1 \leq |b|$ e $|a| > 0$ temos que $|a| \leq |a| \cdot |b|$. Ou seja, $(\mathbb{Z}, +, \cdot, |\ \ |)$ é um domínio Euclidiano.

Exemplo 2. Seja K um corpo e seja $\psi: K\backslash\{0\} \longrightarrow \mathbb{N}$ a função nula. Então, dados $a, b \in K, b \neq 0$ existem $q = ab^{-1}$ e $r = 0$ tais que $a = bq + r$ e $r = 0$. Além disto, se $a, b \in K\backslash\{0\}$, então $|a| = 0 \leq 0 \cdot 0 = |a| \cdot |b|$. Logo, $(K, +, \cdot, \psi)$ é um domínio euclidiano.

Exemplo 3. Seja $D = \mathbb{Z}[i] = \{\alpha = a + bi; a, b \in \mathbb{Z} \text{ e } i = \sqrt{-1}\}$ o subdomínio dos complexos formados pelos números que têm partes real e imaginária inteiras (Este domínio é conhecido como o anel dos inteiros gaussianos).

Seja $f: \mathbb{C} \longrightarrow \mathbb{R}_+$, dada por $f(z) = |z|^2$ que evidentemente, é multiplicativa, isto é, $f(z_1 \cdot z_2) = f(z_1) \cdot f(z_2)$ e seja $N: \mathbb{Z}[i] \longrightarrow \mathbb{N}$ a função restrição de f a $\mathbb{Z}[i]$ com contradomínio $\mathbb{N}$. Então, $\forall \alpha, \beta \in \mathbb{Z}[i], N(\alpha\beta) = N(\alpha) \cdot N(\beta)$ e $N(\alpha) = 0 \Leftrightarrow \alpha = 0$.

Afirmação.$(\mathbb{Z}[i], +, \cdot, N)$ é um domínio euclidiano. Com efeito, sejam $\alpha, \beta \in \mathbb{Z}[i]$ onde $\beta \neq 0$. Vamos exibir $\gamma, \delta \in \mathbb{Z}[i]$ tais que $\alpha = \beta\gamma + \delta$ e $\delta = 0$ ou $N(\delta) < N(\beta)$. Escrevendo $\delta = \alpha - \beta\gamma = \beta\left(\frac{\alpha}{\beta} - \gamma\right)$ com $\frac{\alpha}{\beta} \in \mathbb{C}$, temos $f(\delta) = f(\beta) \cdot f\left(\frac{\alpha}{\beta} - \gamma\right)$, ou seja, $N(\delta) = N(\beta) \cdot f\left(\frac{\alpha}{\beta} - \gamma\right)$.

Agora sejam $x, y \in \mathbb{Q}$ tais que $\frac{\alpha}{\beta} = x + yi$ e sejam $a, b \in \mathbb{Z}$ tais que $|x - a| \leq \frac{1}{2}$ e $|y - b| \leq \frac{1}{2}$. É fácil ver que estes inteiros existem! Tomemos agora, $\gamma = a + bi$ e $\delta = \alpha - \beta\gamma$. Assim,

$N(\delta) = N(\beta) \cdot \left|\frac{\alpha}{\beta} - \delta\right|^2 =$

$= N(\beta)((x - a)^2 + (y - b)^2) =$

$= N(\beta)(|x - a|^2 + |y - b|^2) \leq N(\beta)\left(\frac{1}{4} + \frac{1}{4}\right) =$

$= N(\beta) \cdot \frac{1}{2} < N(\beta).$

Portanto, existem $\gamma, \delta \in \mathbb{Z}[i]$ tais que $\alpha = \beta\gamma + \delta$ e $N(\delta) < N(\beta)$. Notemos que esta última igualdade é equivalente a $N(\delta) = 0$ ou $N(\delta) < N(\beta)$.

Finalmente, dados $\alpha, \beta \in \mathbb{Z}[i]\backslash\{0\}$, temos $1 \leq N(\beta)$ e $N(\alpha) > 0$ de modo que $N(\alpha) \leq N(\alpha) \cdot N(\beta)$.

Notemos que a escolha de γ e δ como fizemos não garante a unicidade do par γ, δ. No caso de $\alpha = \frac{1}{2} + \frac{1}{2}i$ e $\beta = 1, \frac{\alpha}{\beta} = \alpha$. Neste caso $\gamma = a + bi$ deve ser tal que $\left|\frac{1}{2} - a\right| \leq \frac{1}{2}$ e $\left|\frac{1}{2} - b\right| \leq \frac{1}{2}$.

Podemos escolher a e b no conjunto $\{0, 1\}$ ou seja, γ pode ser $0, 1$ ou i.

Proposição 1. Todo domínio euclidiano é principal.

Demonstração.

Sejam D um domínio euclidiano e I um ideal não nulo de D. Sejam $X = \{\psi(a); a \in I\backslash\{0\}\}$ e $d = mín\, X$. Então o ideal $dD \subset I$. Seja $a \in I$ e sejam $q, r \in D$ tais que $a = dq + r$ onde $r = 0$ ou $\psi(r) < \psi(d)$. Como $r = a - dq \in I$ e $\psi(r) < \psi(d)$ temos que $r = 0 \Longrightarrow a = dq$ e $I \subset dD$. Portanto $I = dD$.

Sejam $a_1, a_2, a_3, \dots, a_n$ elementos de um domínio euclidiano O, não todos nulos. Um elemento $d \in D$ tal que $(a_1, a_2, a_3, \dots, a_n) = (d)$ cumpre as seguintes condições:

i) $d | a_1, a_2, a_3, \dots, a_n$
ii) Existem $b_1, b_2, b_3, \dots, b_n \in D$ tais que $a_1b_1 + a_2b_2 + a_3b_3 + \dots + a_nb_n = d$
iii) Se existe $d' \in D$ tal que $d' | a_1, a_2, a_3, \dots, a_n$ então $d' | d$.

Portanto, d é um máximo divisor comum de $a_1, a_2, a_3, \dots, a_n$.

Para o cálculo de um máximo divisor comum, podemos usar o algoritmo de Euclides, das divisões sucessivas em todo domínio euclidiano.

Exemplo 4. Vamos em $\mathbb{Z}[i]$, calcular um máximo divisor comum dos elementos $\alpha = 3 + 2i$ e $\beta = 2 + i$. Façamos:

	$1+i$	$1+i$	$-2+i$
$3+2i$	$2+i$	$2-i$	-1
	$2-i$	-1	0

$\Rightarrow -1$ é um máximo divisor comum de $3 + 2i$ e $2 + i$ em $\mathbb{Z}[i]$.

Observação. Vejamos na atividade 1 que $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$. Logo, cada ideal não nulo de $\mathbb{Z}[i]$ tem quatro geradores e é fácil ver que em cada quadrante do plano complexo, tem um destes geradores. Dados $a_1, a_2, a_3, \dots, a_n \in \mathbb{Z}[i]$ não todos nulos, escolhemos, por definição, um dos máximos divisores comuns, para ser "o máximo divisor comum" aquele d que está no primeiro quadrante. O indicaremos por $mdc(a_1, a_2, a_3, \dots, a_n)$. Precisamente, $d = mdc(a_1, a_2, a_3, \dots, a_n)$ ou $(d) = (a_1, a_2, a_3, \dots, a_n)$, $Re\ d > 0$ e $\mathrm{Im\ d} \geq 0$. Por exemplo, $mdc(3 + 2i, 2 + i) = (-1) \cdot (-1) = 1$.

Exemplo 5. Seja $\omega = cos\frac{2\pi}{3} + i\ sen\frac{2\pi}{3}$ e $D = \mathbb{Z}[\omega] = \{\alpha = a + b\omega; a, b \in \mathbb{Z}\}$. É fácil ver que $\mathbb{Z}[\omega]$ é um subdomínio do corpo dos números complexos. Para cada $\alpha = a + b\omega$, notemos que $|\alpha|^2 = \alpha \cdot \overline{\alpha} = (a + b\omega)\left(\overline{a + b\omega}\right) = (a + b\omega)(a + b\overline{\omega}) = a^2 + ab\overline{\omega} + ab\omega + b^2\omega\overline{\omega}$

Notando que $\overline{\omega} + \omega = -1$ e $\omega \cdot \overline{\omega} = 1$ temos que $|\alpha|^2 = a^2 - ab + b^2$.

Consideremos a função $N: \mathbb{Z}[\omega] \longrightarrow \mathbb{N}$ dada por $N(\alpha) = N(a + b\omega) = a^2 - ab + b^2$. Claramente N é multiplicativa, ou seja, $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$. Vamos provar que $(\mathbb{Z}[\omega], +, \cdot, N)$ é um domínio euclidiano.

Afirmação: Dados $\alpha, \beta \in \mathbb{Z}[\omega]$, onde $\omega \neq 0$, existem γ e $\delta \in \mathbb{Z}[\omega]$ tais que $\alpha = \beta\gamma + \delta$ e $\delta = 0$ ou $N(\delta) < N(\beta)$. Se $\alpha, \beta \in \mathbb{Z}[\omega] \setminus \{0\}$, então $N(\alpha) \leq N(\alpha) \cdot N(\beta)$.

De fato, queremos encontrar γ e δ tais que $\alpha = \beta\gamma + \delta$ e $\delta = 0$ ou $N(\alpha) < N(\beta)$. Escrevendo $\delta = \alpha - \beta\gamma = \beta\left(\frac{\alpha}{\beta} - \gamma\right)$ e $\frac{\alpha}{\beta} = x + iy$ com $x, y \in \mathbb{R}$, como fizemos no caso dos inteiros gaussianos, tomemos $a, b \in \mathbb{Z}$ tais que $|x - a| \leq \frac{1}{2}$ e $|y - b| \leq \frac{1}{2}$, façamos $\gamma = a + b\omega$ e $\delta = \alpha - \beta\gamma$. Agora, $N(\delta) = N(\beta) \cdot \left|\frac{\alpha}{\beta} - \gamma\right|^2 = N(\beta) \cdot |(x - a) + (y - b)\omega|^2 \Rightarrow \frac{N(\delta)}{N(\beta)} = (x - a)^2 - (x - a)(y - b) + (y - b)^2 \leq |x - a|^2 + |x - a| \cdot |y - b| + |y - b|^2 \leq \frac{1}{4} + \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{4} < 1$Ou seja, $N(\delta) < N(\beta)$.

Portanto, dados $\alpha, \beta \in \mathbb{Z}[\omega]$ com $\beta \neq 0$, existem γ e δ (não necessariamente únicos) tais que $\alpha = \beta\gamma + \delta$ e $N(\delta) < N(\gamma)$. Notando que $N(\alpha) = 0 \Leftrightarrow \alpha = 0$, temos que para $\alpha, \beta \in \mathbb{Z}[\omega] \setminus \{0\}, 1 \leq N(\beta)$ e que $N(\alpha) > 0$ de modo que $N(\alpha) \leq N(\alpha) \cdot N(\beta)$. Podemos então concluir que $(\mathbb{Z}[\omega], +, \cdot, N)$ é um domínio euclidiano.

Observação. Outro exemplo de domínio euclidiano é o dos polinômios em uma única indeterminada (variável) sobre um corpo que será estudado no curso de Estruturas Algébricas II.

RESUMO

Nesta aula, estudamos os domínios euclidianos, dos quais, os inteiros é um exemplo. Vimos também que todo domínio euclidiano (DE) é um domínio de ideais principais e exibimos dois domínios euclidianos $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$.

ATIVIDADES

1. Sejam D um domínio euclidiano, $a, b, c, d \in D$ não nulos, u um mdc de a e b e v um mdc de c e d. Prove que u e v são associados.
2. Prove que $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$ não são corpos.
3. Determine todos os invertíveis de $\mathbb{Z}[i]$ e os de $\mathbb{Z}[\omega]$.
4. Seja α um elemento primo de $\mathbb{Z}[i]$, prove que existe um elemento primo de $\mathbb{Z}$ tal que $\alpha|p$.
5. Se $\alpha \in \mathbb{Z}[\omega]$ é tal que $N(\alpha)$ é um elemento primo de $\mathbb{Z}$, prove que α é um elemento primo de $\mathbb{Z}[\omega]$.
6. Seja $D = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Z}\}$. Prove que este subdomínio de $\mathbb{R}$, munido da aplicação $\psi: D \longrightarrow \mathbb{N}$ dada por $\psi(a + b\sqrt{2}) = |a^2 - 2b^2|$ é um domínio euclidiano.

COMENTÁRIO DAS ATIVIDADES

Se você, caro aluno, fez a primeira atividade, você deve ter notado que se trata do lema crucial que usamos no cálculo do máximo divisor comum por divisões sucessivas (de Euclides). Basta provar que $u|v$ e $v|u$.

Na segunda questão, dado $\alpha \neq 0$, você deve ter notado que a equação $\alpha x = 1$ nem sempre tem solução no domínio.

Na terceira atividade, você deve ter observado que α é invertível se, e somente se, $N(\alpha) = 1$.

Na quarta atividade, você deve ter notado que $N(\alpha) = \alpha \cdot \overline{\alpha}$ e usado o fato de que α é um elemento primo.

Na quinta, você não deve ter tido dificuldades, pois, $N(\alpha) = \alpha \cdot \overline{\alpha}$.

Na sexta atividade, você deve ter imitado as demonstrações feitas na aula de que $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$ são domínios euclidianos.

REFERÊNCIAS

GONÇALVES, Adilson. Introdução à álgebra. 5. ed. Rio de Janeiro: IMPA, 2007. 194 p. (Projeto Euclides) ISBN.

HUNGERFORD, Thomas W. Abstract algebra: an introduction. 2nd. ed. Austrália: Thomson Learning, ©1997.

GARCIA, Arnaldo; LEQUAIN, Yves. Elementos de álgebra. 3. ed. Rio de Janeiro: IMPA, 2005. 326 p. (Série: Projeto Euclides).